Migrasi Autentikasi dari Pam ke LDAP di Universitas Kristen Petra

Julio Christian Salim, Justinus Andjarwirawan, Henry Novianus Palit
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jln. Siwalankerto 121-131 Surabaya 60236
Telp. (031)-2983455, Fax. (031)-8417658
julio.christiansalim@hotmail.com, justin@petra.ac.id, hnpalit@petra.ac.id

ABSTRAK

Autentikasi di Universitas Kristen Petra menggunakan akun yang disimpan di *local user* sistem operasi yang ada di *server* John dan Peter. Pihak Puskom juga perlu menyimpan lebih banyak data akun yang disimpan. Oleh karena itu, LDAP digunakan untuk menggantikan penyimpanan akun di *local user* sistem operasi. Aplikasi melakukan autentikasi menggunakan PAM melalui dovecot / POP3.

Pengerjaan skripsi berfokus pada implementasi LDAP di Universitas Kristen Petra dan migrasi akun dan aplikasi. Implementasi dan migrasi menggunakan data akun yang disimpan di *server* John dan Peter. Aplikasi yang dibuat untuk melakukan pencarian dan pengaturan akun yang sudah ada maupun membuat akun baru. Aplikasi dibuat untuk mendukung kebutuhan puskom.

Berdasarkan Pengujian yang dilakukan, migrasi akun berhasil dilakukan. Percobaan migrasi dilakukan menggunakan beberapa akun milik mahasiswa dan dosen. Kebutuhan waktu *response time* yang dibutuhkan apabila melakukan autentikasi langsung ke LDAP lebih singkat dibandingkan autentikasi ke POP3.

Kata Kunci : Migrasi, LDAP, PAM , POP3, Linux Debian, Autentikasi Aplikasi, Manajemen Akun

ABSTRACT

Authentication at Petra Christian University using an account that is stored in the local user operating system on the server John and Peter. Puskom need to store more data than it currently can. Therefore, LDAP is used to replace the local user account on the storage operating system. Existing application uses PAM through dovecot / POP3 to authenticate.

Work on the thesis focuses on the implementation of LDAP at Petra Christian University and migration of accounts and applications. Implementation and migration using account data that is stored on a server John and Peter. Applications are made for searching and modify existing account or create new account. Applications are made to support the needs Puskom.

Based on testing performed, the account migration is successful. Testing the migrated account was performed using multiple accounts belongs to students and lecturer. Also response time that is needed by LDAP to authentication request is shorter than autentication using existing system which use POP3.

Keywords: *Migration, LDAP, PAM, POP3, Debian Linux, Application Authentication, Account Management*

1. PENDAHULUAN

Saat ini Universitas Kristen Petra menggunakan PAM (*Pluggable Authentication Module)* untuk semua *user*. PAM menggunakan *local user* di Linux.

Jika sistem autentikasi dengan *local user* tetap digunakan, sistem operasi yang digunakan untuk *server* autentikasi akan sulit untuk diperbarui, hal ini berpotensi menyebabkan masalah keamanan, masalah kompatibilitas dengan metode autentikasi yang lebih baru. Karena PAM / *local user* di Linux Debian juga tidak menyimpan banyak informasi mengenai *user*.

Pihak Pusat Komputer Universitas Kristen Petra membutuhkan sistem autentikasi yang dapat menyimpan lebih banyak informasi dari masing – masing *user* dan lebih mudah untuk melakukan migrasi *user*.

LDAP digunakan untuk memudahkan migrasi. Karena LDAP menyediakan cara untuk melakukan *export user* sehingga lebih mudah untuk dipindah ke *server* LDAP lainnya. *Server* LDAP juga tidak terikat dengan sistem operasi yang digunakan. Sebagai contoh *server* LDAP yang berjalan di Debian dan Ubuntu tidak berbeda, yang terpenting adalah versi dari LDAP. Di LDAP informasi *user* yang disimpan juga fleksibel, karena atribut di *user* bisa dibuat sesuai dengan kebutuhan. LDAP juga memiliki *library* untuk bahasa pemrograman PHP yang memudahkan dalam pembuatan cara autentikasi untuk aplikasi *web* di masa depan. LDAP sendiri secara *default* mengirim pesan autentikasi dengan format *plaintext*, namun LDAP memiliki fasilitas dimana pesan yang dikirim bisa dienkripsi menggunakan TLS (*Transport Layer Security*)/SSL dengan nama LDAPS. LDAP juga bersifat *Platform Neutral* yang berarti LDAP tidak melekat pada sistem operasi tertentu. *Server* LDAP bisa berjalan di berbagai macam sistem operasi.

2. LANDASAN TEORI

2.1. PAM

PAM adalah mekanisme integrasi beberapa skema autentikasi *low-level* ke API (*Application Programming Interface*) *high-level*. Pada Linux Debian, PAM menggunakan data *local user* sebagai *database user*. Data *local user* di Linux Debian disimpan di /etc/passwd dan /etc/shadow. Dengan PAM, aplikasi – aplikasi dapat melakukan autentikasi ke data *local user* yang ada di /etc/passwd dan /etc/shadow.

Dalam pengaturan PAM ada 4 konteks yang bisa diatur, yaitu *auth, account, password, session.* Tiap konteks memiliki fungsi yang berbeda – beda. Sedangkan dalam pengaturan konteks – konteks tersebut ada 6 *control flag* yang bisa digunakan sesuai dengan kebutuhan PAM yaitu *required, requisite, sufficient, optional, include, substack*. *Control flag* tersebut juga memiliki fungsi yang berbeda, namun *feedback* yang didapatkan dari *control flag* tidak dikeluarkan apa adanya. Sebagai contoh apabila hasil dari *control flag* adalah "PAM_ACCT_EXPIRED" maka oleh PAM hanya dianggap sebagai "*failure*".[6]

PAM mengurangi kompleksitas autentikasi, karena *system administrator* bisa menggunakan *database user* yang sama untuk semua *Login* di sistem. *Service* yang sering digunakan di Linux seperti SSH (*Secure Shell*), FTP (*File Transfer Protocol*), TELNET bisa langsung menggunakan data *local user* yang ada di sistem operasi.[3]

2.2. LDAP

LDAP adalah protokol jaringan yang menggunakan *directory* untuk menyimpan data *user*. LDAP dibuat sebagai *general purpose directory server* yang berarti LDAP tidak dibuat untuk menyimpan data tertentu, melainkan data yang disimpan lebih fleksibel dan bisa disesuaikan dengan kebutuhan. Untuk membedakan data *user* yang serupa dalam *directory*, LDAP menggunakan DN (*Distinguished Name*) contoh : "ou=contoh, dc=example, dc=com".[1]

Directory dan *general purpose database* sering dianggap sama, namun sebenarnya *directory* adalah *database* yang memiliki beberapa karakteristik yang membedakan dari *relational database*. Salah satu karakteristik yang dari *directory* adalah *directory* lebih sering diakses untuk *read* dan *search* dibandingkan *update*. *Directory* secara relatif menyimpan data yang bersifat statis, yang tidak sering terjadi perubahan. Kebanyakan *database* menggunakan metode akses *Structured Query Language* (SQL), sedangkan *directory* menggunakan metode akses yang lebih sederhana. [1]

Libraries yang digunakan oleh OpenLDAP bernama libldap. Libldap API mendukung fungsi OpenLDAP yang menggunakan protokol TCP, SSL dan IPC. [8]

2.3. Migrasi PAM ke LDAP

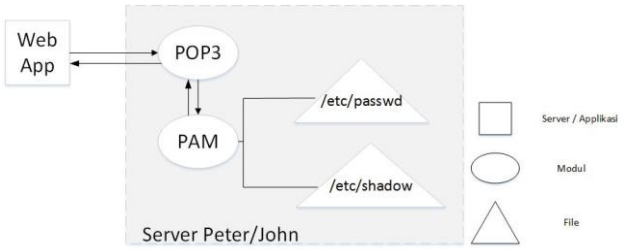
Dalam melakukan migrasi, data *user* diambil dari *local user* yang ada di *file* /etc/passwd dan /etc/shadow. Dari *file* /etc/passwd yang diambil adalah *username*, nama lengkap, dan melihat apakah ada *password*. *Password* dari *username* didapatkan dari *file* /etc/shadow. *Password* yang ada di *file* /etc/shadow sendiri merupakan merupakan *hash* bukan *plaintext*.

2.4. Universitas Kristen Petra

Universitas Kristen Petra saat ini menggunakan PAM yang menggunakan *local user* di Debian untuk autentikasi *user* pada aplikasi – aplikasi *web* yang sudah ada. PAM tersebut berjalan menggunakan sistem operasi Linux Debian 5. Data *user* dibedakan menjadi 2 yaitu Peter dan John. Peter menyimpan data *user* dosen dan pegawai, sedangkan John menyimpan data *user* mahasiswa. John dan Peter berjalan di *server* yang berbeda. Data *user* yang disimpan oleh Universitas Kristen Petra adalah nama lengkap, *username*, dan *password*.

Password user Universitas Kristen Petra dienkripsi oleh Linux Debian menggunakan metode enkripsi MD5 dengan *salt*.

Gambar 1 menggambarkan cara aplikasi melakukan autentikasi. Di Universitas Kristen Petra, aplikasi *web* melakukan autentikasi melalui POP3 yang kemudian akan melakukan autentikasi menggunakan PAM. Hal ini dilakukan agar PAM bisa digunakan untuk autentikasi *User*.



Gambar 1. Kondisi Autentikasi POP3 di Universitas Kristen Petra

2.5. VMware ESXi

Vmware ESXi adalah *Hypervisor* tipe 1. Dimana *Hypervisor* tipe 1 berjalan langsung di atas *hardware*, tidak seperti *Hypervisor* tipe 2 yang berjalan di atas sistem operasi. Hal ini menjanjikan performa yang lebih baik dibandingkan *Hypervisor* tipe 2. Menunjukkan perbedaan antara *Hypervisor* tipe 1 dan tipe 2.

Dalam menentukan *platform* untuk Vmware ESXi harus memperhitungkan kompatibilitas dengan perangkat keras, karena dibandingkan dengan sistem operasi lain (Windows, Linux, Mac OS), Vmware ESXi tidak mendukung semua *storage controller* atau *network adapter chipset* yang ada di pasaran.[5]

2.6. Linux Debian

Linux Debian adalah sistem operasi komputer yang bekerja dengan cara yang mirip dengan sistem UNIX. Linux Debian pertama diumumkan pada tahun 1993 oleh Ian Murdock dan dirilis pertama kali pada tahun 1994. Linux Debian banyak digunakan sebagai sistem operasi *server* memiliki fokus di sisi keamanan dan stabilitas. [4]

Linux Debian tidak dikembangkan oleh sebuah perusahaan, melainkan oleh ribuan *developer* yang memilih kepala proyek setiap 2 tahun.[2]

Debian menggunakan distribusi Linux "DPKG". Menurut Pollei [7] , Linux memiliki 3 distribusi besar, yaitu SLS, RPM, dan DPKG. Menurut Negus dan bresnahan [6], Banyak distro Linux yang berasal dari Debian, jumlahnya diperkirakan sebanyak 120 distro Linux.

3. ANALISA DAN DESAIN SISTEM

3.1. Analisa dan Desain Server LDAP

3.1.1. Sistem Awal

Sistem awal yang dimiliki oleh Universitas Kristen Petra menggunakan 2 *server* yaitu John dan Peter yang memiliki fungsi utama untuk autentikasi. Sistem awal menggunakan Dovecot yang merupakan aplikasi *email* untuk dapat memanfaatkan protokol POP3 untuk autentikasi dari aplikasi *web* ke *local user server* John dan Peter.

Sistem operasi yang berjalan pada *server* John dan Peter adalah Linux Debian 5. Sistem operasi tersebut sudah tidak dapat menerima pembaharuan. Sehingga apabila ada celah keamanan, maupun kekurangan, pihak puskom tidak dapat melakukan pembaharuan.

3.1.2. Hash Password Akun

Hash password akun di *database* LDAP 2.4.40 secara *default* menggunakan metode SSHA (*salted secure hash algorithm*).

Karena metode *hash* yang digunakan untuk penyimpanan *password* akun di Universitas Kristen Petra adalah MD5 dengan *salt*, setiap kali pengguna melakukan autentikasi ke *server* LDAP menggunakan aplikasi *web* manajemen akun, *hash password* akun pengguna akan diubah ke MD5. Perubahan *hash password* saat autentikasi tidak berlaku untuk aplikasi selain aplikasi manajemen akun. Hal ini dilakukan dengan cara melakukan pengecekan *hash password* akun.

3.1.3. Pembagian server fisik ke VM (Virtual Machine)

Dalam proses pembuatan skripsi, penulis menggunakan 2 *server* LDAP. 2 *server* tersebut awalnya digunakan untuk LDAP, namun seiring berjalannya pembuatan skripsi, *server* ldap2.petra.ac.id berfungsi sebagai *server* percobaan dan menyimpan replika aplikasi *web* dari Universitas Kristen Petra. Sedangkan *server* ldap.petra.ac.id digunakan sebagai *server* LDAP utama. Kedua server memiliki sumber daya yang serupa.

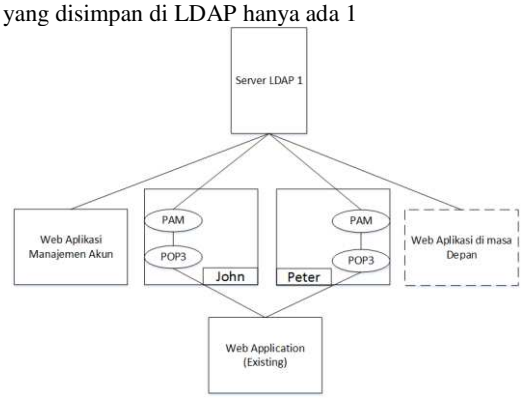
Kedua *server* menggunakan sistem operasi yang sama dan menggunakan *server host* fisik yang sama.

3.1.4. Desain Sistem 1

Pada rancangan desain awal, *server* LDAP dibagi menjadi 2. *Server* pertama menyimpan data hasil migrasi yang memiliki *password* dengan metode *hash* MD5 dan *server* kedua menyimpan data akun yang sudah menggunakan SSHA sebagai metode *hash password*. Namun dengan pertimbangan kemudahan pengaturan, mengurangi kebingungan dalam pengembangan aplikasi di masa yang akan datang dan pergantian *hash password* dapat dilakukan dalam 1 *server* LDAP secara langsung, maka rancangan desain 2 *server* LDAP tersebut dibatalkan.

Gambar 2 menunjukkan skema desain dengan 1 *server* LDAP. Desain ini dipilih dengan beberapa alasan yaitu:

1. VM yang diperlukan hanya 1
2. Lebih mudah dalam pengaturan data akun karena data akun yang disimpan di LDAP hanya ada 1



Gambar 2. Skema desain dengan 1 *server* LDAP dengan libpam-ldap

Desain ini menggunakan sebuah *library* libpam-ldapd pada Debian 8 atau libpam-ldap dan libnss-ldap pada Debian 5. Library tersebut berguna untuk membuat PAM melakukan autentikasi ke LDAP dengan bantuan sebuah *package* lain bernama NSCD (*Name Service Cache Daemon*). NSCD berfungsi sebagai *cache* menyimpan data dari /etc/passwd, /etc/group, dan *server* LDAP agar saat pengguna melakukan autentikasi, *server* yang menjadi penengah (*server* John dan Peter) tidak perlu selalu membuat koneksi ke LDAP dan mengambil data informasi mengenai akun setiap kali ada yang melakukan autentikasi.

3.1.5. Desain Sistem 3

Kedua desain sistem yang sudah di jelaskan tidak digunakan karena ada masalah dengan NSCD yang di instal bersama dengan libpam-ldap dan libnss-ldap. Untuk menghindari gangguan pada *server* John dan Peter di masa depan, penulis melakukan perubahan desain menjadi 1 *server*. Modifikasi pada Dovecot dilakukan untuk melakukan autentikasi ke LDAP apabila autentikasi ke PAM gagal.

3.1.6. Desain jaringan

Server LDAP menggunakan jaringan yang sudah ada di Universitas Kristen Petra. *Server* LDAP diletakkan di ruangan server Pusat Komputer Universitas Kristen Petra yang berada di gedung W.

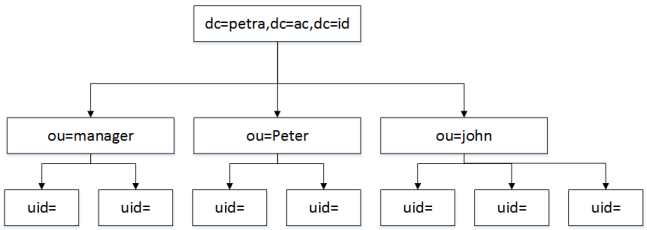
3.1.7. Spesifikasi komputer

Komputer merupakan dasar dari penelitian ini. Komputer dipersiapkan pertama-tama dengan melakukan pembuatan VM dengan Hypervisor tipe 1 yaitu VMWare ESXi. Di VM tersebut dilakukan installasi Linux Debian 8. Linux Debian 8 digunakan karena Debian 8 merupakan versi terbaru dari Linux Debian dan Universitas Kristen Petra sebelumnya juga menggunakan Linux Debian. Setelah Installasi sistem operasi selesai dilakukan, installasi LDAP dan *tools* dilakukan. VM tersebut dibuat dengan spesifikasi sebagai berikut:

Processor	: 1 Core
Memory RAM	: 2GB
Storage	: 100GB

3.2. Desain Directory Information Tree dan LDAP

Pembagian *Sub Tree* ditunjukkan pada gambar 3. Akun dibagi ke 3 OU yang berbeda yaitu John, Peter, dan manager untuk memudahkan pengaturan.



Gambar 3. *Directory Tree* LDAP

3.3. Desain Aplikasi

Aplikasi untuk pengaturan dibuat menggunakan bahasa pemrograman PHP. PHP memiliki *library* untuk mengakses *server* LDAP baik untuk autentikasi maupun pengaturan *user* yang ada di sebuah *server* LDAP.

Aplikasi *web* yang dibuat dapat melakukan sebagai berikut:

- Membuat akun baru untuk akun john dan akun peter oleh *admin*

- Mengubah isi data akun tersebut meliputi *password* dan memperbaiki nama, departemen, dan nomor telepon *extension* oleh pengguna dan *admin*
- Menghapus akun yang sudah tidak digunakan baik menggunakan CSV untuk akun John atau manual satu per satu oleh *admin*
- Pencarian akun berdasarkan nama, user id dan departemen (khusus untuk akun peter) yang dapat dilakukan oleh semua pengguna
- Melakukan *import file* csv untuk pembuatan akun baru John yang dapat dilakukan oleh *admin*

4. IMPLEMENTASI SISTEM

Implementasi dilakukan dengan sistem operasi Debian 8, LDAP, migrasi akun dari *local user server* Peter dan John ke LDAP, konfigurasi Dovecot di *server* Universitas Kristen Petra, aplikasi *web* , dan konfigurasi untuk *server* yang berperan sebagai *client* terhadap *server* LDAP. Konfigurasi LDAP dan migrasi akun menggunakan *script* dengan bahasa perl dan *format file* LDIF. Sedangkan untuk aplikasi *web* menggunakan bahasa pemrograman PHP yang bekerja dengan HTML.

4.1.Instalasi Dan Konfigurasi Sistem Operasi Debian 8

Dalam instalasi sistem operasi ada beberapa nilai yang diminta untuk memenuhi atribut. Atribut tersebut dan nilainya dituliskan pada Tabel 1 Instalasi pada ldap.petra.ac.id dan ldap2.petra.ac.id memiliki atribut instalasi yang serupa. Perbedaan yang dapat dilihat adalah *hostname* di ldap.petra.ac.id menggunakan nilai "ldap" sedangkan di ldap2.petra.ac.id menggunakan nilai "ldap2".

Tabel 1. Atribut Instalasi Sistem Operasi Debian 8

Atribut	Nilai
Hostname	ldap
Domain Name	petra.ac.id
Root Password	**********
Nama untuk *username* baru	justinus
Password username baru	**********
Software yang akan di install	SSH *Server*, *standard system utilities*

4.2.Instalasi Dan Konfigurasi Ldap

Instalasi dan Konfigurasi LDAP dilakukan melalui SSH (*Secure Shell*) menggunakan aplikasi *putty* dari sisi *client*.

Instalasi dan konfigurasi diawali dengan instalasi *package* atau aplikasi yang mendukung LDAP. Lalu dilanjutkan dengan penambahan objectclass dan atribut baru. Agar koneksi dengan TLS dapat dilakukan, sertifikat dan *key* sertifikat di konfigurasi di LDAP. Untuk memenuhi kebutuhan Universitas Kristen Petra yang membutuhkan akun-akun admin dibawah 1 OU (*Organitzational Unit*), maka perubahan terhadap AC (*Access Control*) lalu diakhiri dengan optimalisasi LDAP dengan penambahan indexing.

4.3.Pengisian Database Akun

Migrasi akun mahasiswa, staf, dan dosen yang didapatkan dari *server* John dan Peter milik Universitas Kristen Petra, dilakukan menggunakan *tools* bernama "migrationtools". *Tools* ini digunakan untuk mengubah dara akun John dan Peter ke format yang sesuai dengan LDAP.

Data akun di LDAP dibedakan ke 3 sub-tree yaitu John, Peter dan manager. Agar akun yang sudah di ubah ke format LDAP dapat ditambahkan ke *database* akun LDAP, sub-tree yang belum ada harus ditambahkan ke *database* akun.

Pengisian *database* akun dilakukan menggunakan *file* /etc/passwd dan /etc/shadow yang didapatkan dari *server* John dan *server* Peter. Kedua *file* tersebut digandakan dan diletakkan di *server* LDAP.

Proses pengisian akun dilanjutkan dengan migrasi akun John, akun Peter dan Pembuatan akun manager. Hasil dari migrasi akun John dan akun Peter dimasukkan ke *database* akun menggunakan perintah ldapadd.

4.4.Aplikasi Web

Aplikasi *web* pengaturan akun LDAP diletakkan di ldap.petra.ac.id/ldap. Sedangkan aplikasi yang di migrasi oleh penulis diletakkan di ldap2.petra.ac.id. Agar koneksi dari aplikasi *web* ter-enkripsi, penulis melakukan konfigurasi ke apache untuk HTTPS di ldap.petra.ac.id dan ldap2.petra.ac.id.

Modifikasi yang sama di ldap.petra.ac.id dan ldap2.petra.ac.id. *file certificate* yang diperlukan untuk enkripsi diletakkan di /etc/cert/. *file* pengaturan *web* dilakukan di lokasi /etc/apache2/sites-available/. Di dalam *folder* tersebut ada 2 *file*. *File* pertama adalah default-ssl.conf dan *file* kedua adalah 000-default.conf. *file* pertama digunakan untuk koneksi HTTPS dan *file* kedua digunakan untuk koneksi biasa.

Implementasi dilakukan menggunakan bahasa pemrograman PHP. Aplikasi *web* diletakkan di *server* ldap.petra.ac.id. Tabel 2 menunjukkan *file* utama dalam implementasi aplikasi web manajemen.

Tabel 2. Implementasi Aplikasi Web

Nama File	Proses yang dilakukan
function.php	Koneksi dan autentikasi ke *server* LDAP
	Perubahan *password*
	Pembuatan akun untuk OU John menggunakan CSV
	Penghapusan akun secara individual
	Penghapusan akun menggunakan *file* CSV
	Pembuatan akun untuk OU Peter
schema.php	Pengambilan skema yang ada di *server* LDAP

Migrasi autentikasi aplikasi *web* Universitas Kristen Petra dilakukan pada 2 aplikasi yaitu CSE dan absensi milik jurusan Informatika Universitas Kristen Petra. CSE dapat diakses melalui cse.petra.ac.id sedangkan aplikasi absensi ukpinfor dapat diakses melalui ukpinfor.petra.ac.id. Kedua aplikasi tersebut di migrasi dan diletakkan di ldap2.petra.ac.id. Selain aplikasi, *database* MySQL milik masing-masing aplikasi juga ikut digandakan dan diletakkan di ldap2.petra.ac.id

4.5.Konfigurasi Server Client

Konfigurasi *server* yang bekerja sebagai *client* dari *server* LDAP (contoh: *server* aplikasi *web* yang melakukan autentikasi ke LDAP) diperlukan agar *server client* dapat melakukan koneksi dengan TLS. Koneksi dengan TLS me *encrypt* data / informasi yang keluar dan masuk antara *server* LDAP dan *server client*. Konfigurasi ini perlu dilakukan apabila perlu melakukan autentikasi langsung ke *server* LDAP.

4.5.1. Linux

Untuk sistem operasi Linux dapat dilakukan dengan 2 cara. Cara tersebut adalah :

- Instalasi ldap-utils lalu mengubah isi *file* ldap.conf di /etc/ldap/ dengan menambahkan "TLS_REQCERT never" di bagian paling akhir *file* tersebut.
- Langsung membuat *file* ldap.conf di dalam lokasi /etc/ldap/ dan menambahkan "TLS_REQCERT never" di bagian paling akhir *file* tersebut.

4.5.2. Windows

Untuk sistem operasi Windows yang berperilaku sebagai *server client*, penulis mendapatkan petunjuk dari http://se2.php.net/manual/en/ref.ldap.php tentang lokasi ldap.conf untuk sistem operasi Windows agar dapat membuat koneksi dengan TLS. Pada umumnya lokasi *file* ldap.conf ada di c:\openldap\sysconf\ldap.conf. Untuk isi dari ldap.conf hanya perlu menambahkan "TLS_REQCERT never" di bagian paling akhir.

4.6.Konfigurasi Dovecot

Pada umumnya aplikasi *web* yang ada di Universitas Kristen Petra melakukan autentikasi dengan cara membuka soket koneksi ke *server* John dan Peter dan melakukan autentikasi seperti autentikasi telnet dengan *port* 110 yang tidak di enkripsi.

Dovecot pada awalnya melakukan autentikasi ke *local user*. Namun Dovecot dapat dikonfigurasi untuk melakukan autentikasi ke LDAP. Konfigurasi dilakukan secara langsung pada *server* John dan Peter. *File* konfigurasi *mail server* Dovecot terletak di /etc/dovecot/.

Modifikasi yang dilakukan pada dovecot di *server* John dan Peter adalah untuk menambahkan passdb ldap dan userdb ldap serta melakukan modifikasi pada *file* dovecot-ldap.conf di kedua *server* tersebut.

5. PENGUJIAN SISTEM

Menjelaskan pengujian meliputi kinerja *server* LDAP, *web* aplikasi, dan kompatibiltas autentikasi aplikasi yang sudah ada. Pengujian aplikasi *web* dilakukan melalui 2 tahap yaitu pengujian *user interface* dan sistem penambahan akun baru untuk akun mahasiswa, staf dan dosen.

5.1.Kinerja Server

Pengujian kinerja *server* saat menghadapi proses autentikasi dilakukan menggunakan aplikasi *web* yang dibuat untuk hanya melakukan autentikasi ke *server* LDAP dan POP3 milik Universitas Kristen Petra. Aplikasi *web* tersebut diletakan di *server* ldap2.petra.ac.id untuk mensimulasikan aplikasi *web* milik Universitas Kristen Petra melakukan autentikasi.

Aplikasi *web* pengujian memiliki 1 halaman utama yaitu index.php, 3 halaman berisi fungsi-fungsi yang digunakan untuk pengujian yaitu function.php, ldap.php, pop3.php.

Fungsi-fungsi yang dijalankan di halaman index.php berfungsi untuk langsung melakukan autentikasi. Setiap autentikasi selesai dilakukan, hasil *response time* akan ditulis ke *file* sesuai dengan fungsi yang berjalan

Hasil dari percobaan adalah autentikasi langsung ke LDAP tanpa koneksi TLS memiliki *response time* paling rendah. Disusul oleh autentikasi langsung ke LDAP dengan koneksi TLS. Sedangkan autentikasi ke dovecot menggunakan POP3 membutuhkan waktu yang lebih lama dibandingkan autentikasi ke LDAP dengan koneksi TLS. Begitu juga dengan autentikasi ke POP3 yang kemudian diarahkan ke LDAP.

5.2.Pengujian Web Aplikasi

5.2.1. Pengujian Kompatibilitas Autentikasi Aplikasi Replika

Pengujian autentikasi replika aplikasi hasil migrasi dari Universitas Kristen Petra dilakukan pada aplikasi absensi ukpinfor dan aplikasi cse. Kedua aplikasi tersebut diletakkan di ldap2.petra.ac.id. pengujian dilakukan menggunakan akun LDAP "m26412006".

Hasl dari pengujian web aplikasi replika adalah kedua aplikasi berhasil melakukan autentikasi langsung ke LDAP menggunakan akun "m26412006".

5.2.2. Pengujian Fungsi Aplikasi Manajemen Akun

Aplikasi Manajemen memenuhi kebutuhan Universitas Kristen Petra. Pengguna dapat melakukan pencarian akun lain. Pembuatan dan penghapusan akun John dilakukan menggunakan *file* CSV. Perubahan *password* dapat dilakukan oleh pengguna sendiri atau oleh *admin*. Pembuatan akun Peter mengikuti cara kerja pihak Puskom.

5.3.Kompatibilitas Autentikasi Aplikasi Yang Sudah Ada

Percobaan perubahan autentikasi dilakukan pada aplikasi yang sudah ada pada 2 aplikasi yaitu ukpinfor.petra.ac.id dan cse.petra.ac.id. Agar aplikasi dapat melakukan autentikasi langsung ke LDAP, diperlukan sebuah *library* PHP bernama PHP5-ldap. *Library* ini berisi fungsi-fungsi yang diperlukan untuk melakukan autentikasi langsung ke LDAP, melakukan search, dan hal-hal lain. Namun dari percobaan penulis hasilnya adalah autentikasi ukpinfor.petra.ac.id dan soc.petra.ac.id tidak dapat di ganti atau di modifikasi untuk autentikasi ke LDAP secara langsung.

Hal ini dikarenakan sistem operasi yang sudah tidak didukung lagi. Ukpinfor.petra.ac.id dan cse.petra.ac.id menggunakan Linux Debian 5. Sedangkan Linux Debian 5 sudah tidak menerima bantuan atau *update* apapun lagi. Padahal untuk menginstal *library* PHP5-ldap sistem operasi harus di-*update* terlebih dahulu baru dapat melakukan instalasi *library* tersebut. Solusi yang ditemukan adalah memindah aplikasi *web* tersebut dari Linux Debian 5 ke versi Linux yang lebih baru (contoh: Linux Debian 8), agar sistem operasi dapat tetap mendapatkan *update* dan dapat memenuhi kebutuhan *library* PHP nya.

Replika aplikasi CSE awalnya dapat diakses di soc.petra.ac.id, akses SSH untuk mengubah aplikasi cse dilakukan melalui

debianx.petra.ac.id. Penulis menemukan bahwa ada salah satu fungsi bawaan PHP yang tidak bisa berjalan. Fungsi PHP yang tidak bisa berjalan disebabkan oleh versi dari PHP yang ada di *host* aplikasi tersebut ternyata adalah versi dibawah 5.30. PHP di debianx.petra.ac.id tidak dapat di perbaharui karena sistem operasi yang digunakan yaitu Linux Debian 5.

Linux Debian 5 sudah tidak menerima pembaharuan. Sehingga pada *server* Petra yang tidak memiliki

Aplikasi yang sudah ada dapat melakukan autentikasi ke LDAP apabila autentikasi ke PAM gagal karena Dovecot yang ada di *server* John dan Peter sudah diarahkan untuk melakukan autentikasi ke LDAP apabila autentikasi ke *local user* gagal. Kegagalan autentikasi ke *local user* dapat disebabkan kesalahan *username* maupun *password*. Pembatasan tidak dapat dilakukan apabila akun yang ada di *local user* namun gagal autentikasi tidak dilanjutkan autentikasi ke LDAP. Sehingga apabila ada akun yang ada di *local user* di *server* John maupun Peter sama dengan akun yang ada di *database* akun LDAP namun memiliki *password* yang berbeda, pengguna dapat melakukan autentikasi dengan *password* yang ada di LDAP maupun yang ada di *local user server* John atau Peter.

6. KESIMPULAN DAN SARAN

Kesimpulan yang diperoleh dari migrasi autentikasi dari pam ke ldap di Universitas Kristen Petra adalah sebagai berikut:

- Pembuatan skripsi menggunakan 3 VM milik Universitas Kristen Petra
- Tidak semua aplikasi dapat melakukan autentikasi langsung ke LDAP karena tidak memiliki *library* PHP5-ldap
- Migrasi akun dari *local user server* John dan Peter ke LDAP berhasil dilakukan
- OpenLDAP berhasil menerima permintaan autentikasi dari dovecot yang ada di *server* John, *server* Peter, dan aplikasi yang dibuat atau diubah oleh penulis. Juga Membantu menyimpan data yang dibutuhkan untuk proses operasional Puskom
- Aplikasi manajemen akun yang dibuat membantu memudahkan akses ke data akun serta pemilik akun. Aplikasi manajemen akun membantu mempermudah pembuatan akun baru untuk pembuatan akun mahasiswa, staf, dan dosen dan memberi kemampuan perubahan *password* akun yang disimpan di LDAP
- Dari pengujian, OpenLDAP memiliki *response time* yang lebih cepat dibandingkan autentikasi menggunakan dovecot
- Koneksi yang dilakukan ke LDAP dapat menggunakan koneksi dengan TLS, sehingga perpindahan data terenkripsi
- Dari analisa kelayakan migrasi autentikasi, penulis menyimpulkan bahwa migrasi autentikasi dapat dan layak dilakukan secara bertahap.

Saran untuk migrasi autentikasi dari PAM ke LDAP di Universitas Kristen Petra adalah sebagai berikut:

- Autentikasi aplikasi yang sudah ada beberapa dapat langsung melakukan autentikasi ke LDAP
- Koneksi autentikasi dapat menggunakan koneksi yang terenkripsi

7. REFERENSI

[1] Butcher, M. 2007. *Mastering OpenLDAP*. Birmingham: Packt Publishing Ltd.

[2] Cobbaut, P., et al. 2015. *Linux Fundamentals*. URI= http://linux-training.be /linuxfun.pdf

[3] Geisshirt, K. 2007. *Pluggable Authentication Modules*. Birmingham: Packt Publishing Ltd.

[4] Herztog, R. & Mas, R. 2013. *The Debian Administrator Handbook*. Freexian SARL.

[5] Lowe, S., et al. 2014. *Mastering VMware vSphere* 5.5. Inianapolis: John Wiley & Sons, inc.

[6] Negus, C. & Bresnahan, C. 2012. *Linux Bible* (8th *ed*.). Indianapolis: John Wiley & Sons, inc.

[7] Pollei, R.P. 2013. *Debian 7: System Administration Best Practices*. Birmingham: Packt Publishing Ltd.

[8] Winston, R. 2003. *Using libldap, the LDAP Library Client*.URI= http://www.linuxdevcenter.com/pub/a/linux/ 2003/08/14/libldap .html.